日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年 ３月１４日

出 願 番 号
Application Number: 特願２０００－０７１１８３

出 願 人
Applicant (s): シャープ株式会社
日本電信電話株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年 ２月 ９日

特許庁長官
Commissioner,
Patent Office 及川耕造

【書類名】　特許願

【整理番号】　99J04036

【提出日】　平成12年 3月14日

【あて先】　特許庁長官　近藤　隆彦　殿

【国際特許分類】　G06K 19/00

【発明の名称】　１チップマイクロコンピュータ及びそれを用いたＩＣカード

【請求項の数】　8

【発明者】

【住所又は居所】　大阪府大阪市阿倍野区長池町２２番２２号　シャープ株式会社内

【氏名】　若林　正樹

【発明者】

【住所又は居所】　大阪府大阪市阿倍野区長池町２２番２２号　シャープ株式会社内

【氏名】　小川　竜一

【発明者】

【住所又は居所】　大阪府大阪市阿倍野区長池町２２番２２号　シャープ株式会社内

【氏名】　八重川　和宏

【発明者】

【住所又は居所】　大阪府大阪市阿倍野区長池町２２番２２号　シャープ株式会社内

【氏名】　栗岡　進

【発明者】

【住所又は居所】　大阪府大阪市阿倍野区長池町２２番２２号　シャープ株式会社内

【氏名】　大野　謙次

【発明者】

【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

【氏名】　竹田　忠雄

【発明者】

【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

【氏名】　首藤　啓樹

【発明者】

【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

【氏名】　吉沢　正浩

【特許出願人】

【識別番号】　000005049

【氏名又は名称】　シャープ株式会社

【特許出願人】

【識別番号】　000004226

【氏名又は名称】　日本電信電話株式会社

【代理人】

【識別番号】　100080034

【弁理士】

【氏名又は名称】　原　謙三

【電話番号】　06-6351-4384

【手数料の表示】

【予納台帳番号】　003229

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　　要約書　1

【包括委任状番号】　9003082

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　１チップマイクロコンピュータ及びそれを用いたＩＣカード

【特許請求の範囲】

【請求項１】

特定アドレス空間を実行しているときに設定可能で、アクセスを許可するアドレス範囲を設定するアクセス許可アドレス範囲設定手段と、

ソフトウェアの実行中に、設定された上記アドレス範囲内でアクセスされているか否かを判断する判断手段と、

上記特定アドレス空間を実行しているときに設定可能で、上記アドレス範囲以外のアドレスのアクセスを許可するか否かを設定するアクセス許可設定手段と、

上記判断手段の結果と上記アクセス許可設定手段の設定内容とに基づいて、メモリに対するアクセスを制御する制御手段とを備えている１チップマイクロコンピュータ。

【請求項２】

特定アドレス空間を実行していることを表すフラグをセットするモニタフラグと、

上記フラグがセットされているときに設定可能で、アクセスを許可するアドレス範囲を設定するアクセス許可アドレス範囲設定レジスタと、

ソフトウェアの実行中に、設定された上記アドレス範囲内でアクセスされているか否かを判断する判断手段と、

上記フラグがセットされているときに設定可能で、上記アドレス範囲以外のアドレスのアクセスを許可するか否かを設定するアクセス許可設定レジスタと、

上記判断手段の結果と上記アクセス許可設定レジスタの設定内容とに基づいて、メモリに対するアクセスを制御する制御手段とを備えている１チップマイクロコンピュータ。

【請求項３】

上記特定のアドレス空間には、システムソフトウェアが格納されており、該システムソフトウェアは、次のプログラムを実行する前に、該プログラムの格納されているアドレス範囲を上記アクセス許可アドレス範囲設定レジスタに設定する

と共に、該アドレス範囲外のアドレスに対してアクセスを許可しないように上記アクセス許可レジスタを設定することを特徴とする請求項２に記載の１チップマイクロコンピュータ。

【請求項４】

上記アドレス範囲外のアドレスのアクセスを不許可とする設定がアクセス許可設定レジスタになされており、上記アドレス範囲外のアドレスに対してアクセスしたことが判断手段によって判断されたとき、割り込み要求信号を生成してＣＰＵへ送る割り込み要求信号生成手段を更に備え、所定の割り込み処理プログラムを実行することを特徴とする請求項２又は３に記載の１チップマイクロコンピュータ。

【請求項５】

上記割り込み処理プログラムは、システムプログラムまたはオペレーティングシステムに制御を移すプログラムであることを特徴とする請求項４に記載の１チップマイクロコンピュータ。

【請求項６】

上記システムソフトウェアが管理する領域に設けられ、メモリへのアクセス制限を越えてアクセスが行われた場合にその旨の情報を記憶する再実行禁止情報記憶手段を更に備え、該情報に基づいて、上記制御手段は上記メモリを制御し、アクセス制限を越えて上記アクセスが再度行われないようにすることを特徴とする請求項３に記載の１チップマイクロコンピュータ。

【請求項７】

上記メモリは、書き換え可能な不揮発性メモリであることを特徴とする請求項１、２、３、４、５、又は６に記載の１チップマイクロコンピュータ。

【請求項８】

請求項１、２、３、４、５、６、又は７に記載の１チップマイクロコンピュータを用いたＩＣカード。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、プログラムメモリに複数のアプリケーションプログラムを搭載した１チップマイクロコンピュータ及びそれを用いたＩＣカードに関し、特にメモリへのアクセスを制限し、アプリケーションプログラム間のデータのセキュリティ性を高めた１チップマイクロコンピュータ及びそれを用いたＩＣカードに関するものである。

【０００２】

【従来の技術】

大容量不揮発性メモリをプログラムメモリとして搭載した１チップマイクロコンピュータは、各種用途に適した複数のアプリケーションプログラムを予めプログラムメモリに書き込んでおき、それぞれのプログラムを選択し実行処理させることがある。

【０００３】

１チップマイクロコンピュータに搭載されている内蔵メモリは、ＣＰＵによってアクセスされるため、同一ＣＰＵで動作するプログラムは、どのプログラムでもＣＰＵのアクセス可能な範囲のデータに対してアクセスできる。この場合、複数のアプリケーションプログラムを搭載していると、一方のアプリケーションプログラムが他方のアプリケーションプログラムの命令コードやデータにアクセスすることができてしまい、他方のアプリケーションプログラムやデータを改ざんできたり、読み出することが可能となり、セキュリティ性を損なうという問題を招来していた。

【０００４】

上記問題の解決手段として、特開平８－５５２０４号公報には、ＣＰＵにプログラムセグメントレジスタとプログラムカウンタとメモリ上のデータをアクセスするためのレジスタとを備え、これらの演算により実行、及び読み書きを行うアドレスを求めてメモリアクセスを制限する方法が開示されている。

【０００５】

このメモリアクセス制限方法を適用したＩＣカードは、図８に示すように、ＣＰＵ１０１と、ＲＯＭ１０２と、ＲＡＭ１０３と、ＥＥＰＲＯＭ１０４とで構成されており、ＣＰＵ１０１の内部構成と機能に上記解決手段が存在している。

【０００６】

そして、図９に示すように、このＣＰＵ１０１には、ＣＰＵ１０１をリセット後、一度だけ値をリセットすることができるプログラムセグメントレジスタ（ＰＳＲ）２０１と、メモリ上のデータをアクセスするためのデータアクセス用オフセットレジスタ（ＤＲ）２０２と、プログラムカウンタ（ＰＣ）２０３及びプログラムセグメントレジスタ２０１に基づいて実行アドレスを生成するアドレス加算手段２０５と、データアクセス用オフセットレジスタ２０２及びプログラムセグメントレジスタ２０１からデータを読み出して書き込みアドレスを生成するアドレス加算手段２０４と、実行アドレスの生成とデータ読み出しアドレス及びデータ書き込みアドレスの生成に共通のオフセットアドレス値を生成するアドレス乗算手段２０６を有している。

【０００７】

なお、上記プログラムセグメントレジスタ２０１は、外部より受け取った目的のアプリケーションプログラムの識別番号を保存しておくために使用される。上記データアクセス用オフセットレジスタ２０２は、読み書きする際のアドレス値にオフセットを持たせるためのオフセット値を格納するために使用される。

【０００８】

また、プログラムカウンタ２０３は、プログラムの実行命令のアドレスを指し示すものである。例えば、外部より受け取った目的のアプリケーションプログラムの識別番号が２の場合には、その数値２がプログラムセグメントレジスタ２０１に保存され、絶対オフセット値として実行するアドレスがプログラムセグメントレジスタの１０００倍に設定されている場合には、プログラム実行アドレスを（２×１０００）番地へ移行する。以降は、実行アドレスが（２×１０００＋プログラムカウンタ２０３の値）番地となるように、プログラムセグメントレジスタ２０１の値とプログラムカウンタ２０３の値とから実行すべきアドレスを指定する。

【０００９】

また、データの読み書きアドレスについては、アドレス（２×１０００＋データアクセス用オフセットレジスタ２０２の値）番地を特定して実行するように、

プログラムセグメントレジスタ２０１の値とデータアクセス用オフセットレジスタ２０２の値から読み書きするアドレスを求める。

【００１０】

上記より、プログラムセグメントレジスタ２０１に格納された目的のアプリケーションプログラムの識別番号で指定されたアプリケーションプログラムを実行している間は、そのアプリケーションプログラムが格納されたアドレス範囲とＲＡＭ以外に対して、アクセスが不可能となる。

【００１１】

したがって、プログラムメモリに複数のアプリケーションプログラムを搭載する場合に、一方のアプリケーションプログラムが他方のアプリケーションプログラムの命令コードやデータにアクセスすることを不可能とし、これにより、セキュリティ性を確保していた。

【００１２】

【発明が解決しようとする課題】

しかしながら、上記従来のアドレス制限方法では、プログラムセグメントレジスタの設定は一度だけという制約から、ＣＰＵのリセット後、一つのアプリケーションプログラムのみ実行可能であり、引き続き他のアプリケーションプログラムを実行するためには、再度、ＣＰＵのリセットが必要である。また、アプリケーションプログラム間において通信ができない等、利便性に問題があった。

【００１３】

例えば、複数のアプリケーションプログラムを搭載したＩＣカードに応用した場合、ＩＣカードをＩＣカードシステム内のリーダライタから切り離した状態、つまり、電源を遮断するまで、他のアプリケーションプログラムが実行できない状態となる。

【００１４】

このため、一連の複数のアプリケーションプログラムを実行させようとした場合、一つのアプリケーションプログラムの実行が終了するたびにＩＣカードをリーダライタから切り離し、再度挿入し、ＩＣカードの初期処理をその度に繰り返す必要が生じ、一連の処理時間が長大化するという問題と、ＩＣカードを何度も

抜き差しする手間が生じるという問題とがあった。

【００１５】

また、現在実行中のアプリケーションプログラム内でサブルーチンコール等を行い、元のアドレスに戻したい場合は、一般的にリターンアドレスが一時的にＲＡＭに格納されるが、この値が不具合で又は故意で別の値に書き変わると、アプリケーションプログラムが暴走したり、その他のアプリケーションプログラムをアクセスしてしまう要因となる可能性がある。結果として、ＣＰＵは、暴走してしまうことになるが、上記アクセス制限方法では、このような場合の対策が一切講じられていない。

【００１６】

そこで、本発明は上記問題点に鑑みなされたものであり、その目的は、複数のアプリケーションプログラムが格納された１チップマイクロコンピュータにおいて、一方のアプリケーションプログラムが他方のアプリケーションプログラムの命令コードやデータにアクセスすることを不可能とし、セキュリティ性を確保した１チップマイクロコンピュータを提供することにある。

【００１７】

本発明の他の目的は、複数のアプリケーションプログラムをリセット動作などを必要とせず連続的に実行できるようにして利便性を向上させることが可能な１チップマイクロコンピュータを提供することにある。

【００１８】

本発明の更に他の目的は、アプリケーションプログラムがプログラムの不具合または故意に他のアプリケーションプログラムにアクセスすることがあっても、ＣＰＵは暴走することなくアクセス制限機能を有効にしたまま処理の継続が行える１チップマイクロコンピュータを提供することにある。

【００１９】

【課題を解決するための手段】

本発明に係る１チップマイクロコンピュータは、特定アドレス空間を実行しているときに設定可能で、アクセスを許可するアドレス範囲を設定するアクセス許可アドレス範囲設定手段と、ソフトウェアの実行中に、設定された上記アドレス

範囲内でアクセスされているか否かを判断する判断手段と、上記特定アドレス空間を実行しているときに設定可能で、上記アドレス範囲外のアドレスのアクセスを許可するか否かを設定するアクセス許可設定手段と、上記判断手段の結果と上記アクセス許可設定手段の設定内容とに基づいて、メモリに対するアクセスを制御する制御手段とを備えている。

【００２０】

上記の発明によれば、特定のアドレス空間に格納されたソフトウェアが実行されているときに、アクセス許可アドレス範囲設定手段及びアクセス許可設定手段の各設定手段に対して設定可能となる。

【００２１】

上記特定のアドレス空間に格納されたソフトウェアが実行されていないときには、たとえ上記特定のアドレス空間から設定しても、アクセス許可アドレス範囲設定手段及びアクセス許可設定手段の各設定手段に対して設定することはできなくなる。

【００２２】

上記特定のアドレス空間に格納されたソフトウェアが実行されているときに、上記特定のアドレス空間からアクセス許可アドレス範囲設定手段を介してアドレス範囲が設定できる。この場合、ソフトウェアの実行中に、該設定されたアドレス範囲内のアドレスに対してアクセスされているか否かが判断手段によって判断される。一方、上記特定のアドレス空間に格納されたソフトウェアが実行されていないときには、いくらデータが上記特定のアドレス空間からアクセス許可アドレス範囲設定手段に入力されていても、該データは該アクセス許可アドレス範囲設定手段に書き込まれることない。

【００２３】

一方、上記特定のアドレス空間に格納されたソフトウェアが実行されているときに、上記特定のアドレス空間からアクセス許可設定手段を介して上記アドレス範囲外のアドレスのアクセスを許可するか否かが設定できる。一方、上記特定のアドレス空間に格納されたソフトウェアが実行されていないときには、いくらデータが上記特定のアドレス空間からアクセス許可設定手段に入力されていても、

該データは該アクセス許可設定手段に書き込まれることない。

【００２４】

上記判断手段の判断結果と、上記アクセス許可設定手段の設定内容とに基づいて、メモリに対するアクセスが制御手段によって制御される。すなわち、アドレス範囲が設定されていて、且つ、アドレス範囲外のアドレスのアクセスが許可されていないときには、メモリにおいて、該アドレス範囲内のアドレスに対してのみアクセス可能となる一方、該アドレス範囲外のアドレスに対してはアクセスはできない。

【００２５】

このようにメモリに対するアクセスを制御することによって、実行中のプログラムが他のプログラムが格納されているアドレス空間に悪影響を及ぼすことを未然に回避できる。また、特定のアドレス空間からのみ、アクセス許可設定手段とアドレス範囲設定手段とに対して設定ができるため、これらの設定手段もアプリケーションプログラムから影響を受けない。つまり、特定アドレス空間からのみアクセス可能なアクセス許可手段、アクセス範囲設定手段に対しても影響を与えない。

【００２６】

なお、アドレス範囲が設定されていて、且つ、アドレス範囲外のアドレスのアクセスが許可されているときには、該アドレス範囲外のアドレスに対してもアクセス可能となる。

【００２７】

本発明に係る他の１チップマイクロコンピュータは、特定アドレス空間を実行していることを表すフラグをセットするモニタフラグと、上記フラグがセットされているときに設定可能で、アクセスを許可するアドレス範囲を設定するアクセス許可アドレス範囲設定レジスタと、ソフトウェアの実行中に、設定された上記アドレス範囲内でアクセスされているか否かを判断する判断手段と、上記フラグがセットされているときに設定可能で、上記アドレス範囲外のアドレスのアクセスを許可するか否かを設定するアクセス許可設定レジスタと、上記判断手段の結果と上記アクセス許可設定レジスタの設定内容とに基づいて、メモリに対するア

クセスを制御する制御手段とを備えている。

【００２８】

上記の発明によれば、特定のアドレス空間に格納されたソフトウェアが実行されているときにフラグがモニタフラグによってセットされる。フラグがセットされているときに、アクセス許可アドレス範囲設定レジスタ及びアクセス許可設定レジスタの各レジスタに対して設定可能となる。

【００２９】

フラグがセットされていないときには、特定のアドレス空間に格納されたソフトウェアが実行されていないので、モニタフラグはフラグをセットしない。したがって、このとき、たとえ上記特定のアドレス空間から設定しても、アクセス許可アドレス範囲設定レジスタ及びアクセス許可設定レジスタの各レジスタに対する設定はできなくなる。

【００３０】

上記フラグがセットされているときに、上記特定のアドレス空間からアクセス許可アドレス範囲設定レジスタを介してアドレス範囲が設定できる。この場合、ソフトウェアの実行中に、該設定されたアドレス範囲内のアドレスに対してアクセスされているか否かが判断手段によって判断される。一方、上記フラグがセットされていないときに、いくらデータが上記特定のアドレス空間からアクセス許可アドレス範囲設定レジスタに入力されていても、該データは該アクセス許可アドレス範囲設定レジスタに書き込まれることない。

【００３１】

これに対して、上記フラグがセットされているときに、上記特定のアドレス空間からアクセス許可設定レジスタを介して上記アドレス範囲外のアドレスのアクセスを許可するか否かが設定できる。一方、上記フラグがセットされていないときには、いくらデータが上記特定のアドレス空間からアクセス許可設定レジスタに入力されていても、該データは該アクセス許可設定レジスタに書き込まれることない。

【００３２】

上記判断手段の判断結果と、上記アクセス許可設定レジスタの設定内容とに基

づいて、メモリに対するアクセスが制御手段によって制御される。すなわち、アドレス範囲が設定されていて、且つ、アドレス範囲外のアドレスのアクセスが許可されていないときには、メモリにおいて、該アドレス範囲内のアドレスに対してのみアクセス可能となる一方、該アドレス範囲外のアドレスに対してはアクセスはできない。

【００３３】

このようにメモリに対するアクセスを制御することによって、実行中のプログラムが他のプログラムが格納されているアドレス空間に悪影響を及ぼすことを未然に回避できる。また、特定のアドレス空間からのみ、アクセス許可設定レジスタとアドレス範囲設定レジスタとに対して設定ができるため、これらのレジスタもアプリケーションプログラムから影響を受けない。つまり、特定アドレス空間からのみアクセス可能なアクセス許可レジスタ、アクセス範囲設定レジスタにも影響を与えない。

【００３４】

なお、アドレス範囲が設定されていて、且つ、アドレス範囲外のアドレスのアクセスが許可されているときには、該アドレス範囲外のアドレスに対してもアクセス可能となる。

【００３５】

上記１チップマイクロコンピュータにおいて、上記特定のアドレス空間には、システムソフトウェアが格納されており、該システムソフトウェアは、次のプログラムを実行する前に、該プログラムの格納されているアドレス範囲を上記アクセス許可アドレス範囲設定レジスタに設定すると共に、該アドレス範囲外のアドレスに対してアクセスを許可しないように上記アクセス許可レジスタを設定することが好ましい。

【００３６】

この場合、次のプログラムが実行されるのに先立って、システムソフトウェアは、この実行しようとしている次のプログラムの格納されているアドレス範囲をアクセス許可アドレス範囲設定レジスタに設定する。つまり、実行中のプログラムは、次に実行するプログラムのアドレス範囲が設定されるまで、該次に実行す

るプログラムをアクセスすることはない。

【００３７】

以上のように、オペレーティングシステムなどのシステムソフトウェアからアプリケーションプログラム等の次に実行されるプログラムへ制御が移行される前に、アクセス可能とするアドレス範囲を設定できる。したがって、実行中のプログラムが次に実行されるプログラムに影響を与えることを未然に回避でき、信頼性が著しく向上する。

【００３８】

上記１チップマイクロコンピュータにおいて、上記アドレス範囲外のアドレスのアクセスを不許可とする設定がアクセス許可設定レジスタになされており、上記アドレス範囲外のアドレスに対してアクセスしたことが判断手段によって判断されたとき、割り込み要求信号を生成してＣＰＵへ送る割り込み要求信号生成手段を更に備え、所定の割り込み処理プログラムを実行することが好ましい。

【００３９】

この場合、他のプログラムによって不正なアクセスがなされたとき、アドレス範囲外のアドレスに対してアクセスしたことが判断手段によって判断され、割り込み要求信号生成手段によって割り込み要求信号が生成されてＣＰＵへ送られる。ＣＰＵは、この割り込み要求信号を受領すると、所定の割り込み処理プログラムが実行されるので、ＣＰＵが暴走することを未然に防ぐことができる。

【００４０】

上記１チップマイクロコンピュータにおいて、上記割り込み処理プログラムは、システムプログラムまたはオペレーティングシステムに制御を移すプログラムであることが好ましい。この場合、割り込み要求信号生成手段によって割り込み要求信号が生成されてＣＰＵへ送られると、割り込み処理プログラムが実行され、システムプログラムまたはオペレーティングシステムに制御が移される。これにより、ＣＰＵまたはアプリケーションプログラムの暴走を防ぐことが可能となる。

【００４１】

上記１チップマイクロコンピュータにおいて、上記システムソフトウェアが管

理する領域に設けられ、メモリへのアクセス制限を越えてアクセスが行われた場合にその旨の情報を記憶する再実行禁止情報記憶手段を更に備え、該情報に基づいて、上記制御手段は上記メモリを制御し、アクセス制限を越えて上記アクセスが再度行われないようにすることが好ましい。

【００４２】

この場合、メモリへのアクセス制限を越えてアクセスが行われると、その旨の情報が再実行禁止情報記憶手段（例えば、フラグやレジスタ等）に記憶されることになる。上記制御手段は、この情報に基づいて上記メモリを制御し、アクセス制限を越えて上記アクセスが再度行われないようにする。これにより、一旦不正なアクセスが行われたプログラムに対しては、それ以降、その実行が禁止されるので、ＣＰＵは、暴走することなく処理を継続して行うことが可能となる。

【００４３】

上記１チップマイクロコンピュータにおいて、上記メモリは、書き換え可能な不揮発性メモリであることが好ましい。この場合、後から追加したり、書き換えたりしたプログラム（例えば、アプリケーションプログラム）等が既存のプログラムに影響を与えることなく実行することができる。

【００４４】

上記の１チップマイクロコンピュータは、ＩＣカードに適用することが好ましい。この場合、複数のアプリケーションプログラムを内蔵したＩＣカードにおいて、アプリケーションプログラム間のセキュリティ性を確実に確保することができる。また、複数のプログラムを格納するＩＣカードを実現でき、それぞれのプログラムをリセットすることなく動的に切り換えることができるので、そのＩＣカードをリーダライタに挿入した状態で多目的に利用できる。さらに、複数のプログラム及びデータ間の干渉を禁止できるため、不正なプログラムのアクセス防止やデータの保護等のセキュリティ性が確保できるので、個人情報等の機密データを格納するＩＣカードに適している。

【００４５】

【発明の実施の形態】

本発明の実施の一形態について図１乃至図７に基づいて説明すれば、以下のと

おりである。

【００４６】

本実施の形態においては、不揮発性メモリを搭載したＩＣカード用１チップマイクロコンピュータに本発明を適用した場合について説明する。

【００４７】

図２は、ＩＣカード用１チップマイクロコンピュータのブロック図を示している。この１チップマイクロコンピュータは、システムプログラムやアプリケーションプログラムを実行するためのＣＰＵ３０１に加えて、システムプログラムやアプリケーションプログラムを格納するための不揮発性メモリ３０３（例えばフラッシュメモリやＥＥＰＲＯＭ等の書き換え可能なメモリ）、ＣＰＵ３０１の作業用のＲＡＭ６、メモリ保護回路５、外部機器と通信を行うためのＵＡＲＴ２、及びタイマ等周辺回路４を備えている。これらのブロックは、ＣＰＵ１が入出力するアドレス線、データ線、データの読み出しや書き込み及びブロック活性化のための制御線などで接続されている。

【００４８】

図１は、図２のブロック図のＣＰＵ３０１、メモリ保護回路５、不揮発性メモリ３０３について詳細に説明するブロック図である。

【００４９】

この１チップマイクロコンピュータは、ＣＰＵ３０１とこれに含まれるプログラムカウンタ（ＰＣ）３０２と、不揮発性メモリ３０３と、モニタフラグ３０４と、後述するアクセス許可アドレス範囲設定レジスタを含むアクセス許可領域検出回路３０６と、アクセス許可設定レジスタ３０７と、アクセス許可アドレス範囲設定レジスタ及びアクセス許可設定レジスタ３０７に対する書き込み信号の発生を制限するレジスタ書き込み制御回路３０５と、不揮発性メモリ３０３に対して読み出し信号の発生を制限するメモリ読み出し制御回路３０９と、不揮発性メモリ３０３に対して書き込み信号の発生を制限するメモリ書き込み制御回路３１０とを有する。

【００５０】

モニタフラグ３０４には、ＣＰＵ３０１から出力されるアドレスバス信号３１

１と命令の第１サイクルを表す命令取り出し信号３０８（フェッチ）が入力される。ここでは、ＣＰＵ３０１が不揮発性メモリ３０３の特定アドレス空間に格納されたオペレーティングシステムなどのシステムソフトウェアを実行しているか否かの判別が行われる。特定アドレス空間を実行しているとき、モニタフラグ３０４からは２値論理のハイレベル（以下、「１」と称す。）が出力される。一方、特定アドレス空間以外を実行しているとき、モニタフラグ３０４からは２値論理のローレベル（以下、「０」と称す。）が出力される。

【００５１】

レジスタ書き込み制御回路３０５には、ＣＰＵ３０１から出力される書き込み基準信号３１２（ライト）と、モニタフラグ３０４の出力であるモニタフラグ出力信号３１４が入力される。書き込み基準信号３１２は、ＣＰＵ３０１が内蔵レジスタや内蔵メモリに書き込みアクセスしたときに出力される信号である。

【００５２】

レジスタ書き込み制御回路３０５では、書き込み基準信号３１２をアクセス許可領域検出回路３０６内のアクセス許可アドレス範囲設定レジスタとアクセス許可設定レジスタ３０７に伝達するか否かの制御を行う。

【００５３】

モニタフラグ３０４の内容が「１」のとき、つまり、上記特定アドレス空間から書き込み動作が発生したときは、書き込み基準信号３１２は、後述するレジスタ書き込み信号３１９として、アクセス許可領域検出回路３０６内のアクセス許可アドレス範囲設定レジスタ（図示しない）とアクセス許可設定レジスタ３０７とにそれぞれ伝達される。これにより、アクセス許可領域検出回路３０６内のアクセス許可アドレス範囲設定レジスタとアクセス許可設定レジスタ３０７への書き込みが可能になる。

【００５４】

これに対して、モニタフラグ３０４の内容がデータ「０」のとき、つまり、特定アドレス空間以外から書き込み動作が発生したときは、書き込み基準信号３１２はアクセス許可領域検出回路３０６内のアクセス許可アドレス範囲設定レジスタとアクセス許可設定レジスタ３０７との何れに対しても伝達されない。これに

より、アクセス許可領域検出回路３０６内のアクセス許可アドレス範囲設定レジスタとアクセス許可設定レジスタ３０７への書き込みは禁止される。

【００５５】

図３は、図１のブロック図におけるアクセス許可領域検出回路３０６、アクセス許可設定レジスタ３０７、メモリ読み出し制御回路３０９、及びメモリ書き込み制御回路３１０との動作について、更に詳細に説明したブロック図である。

【００５６】

アクセス許可領域検出回路３０６には、ＣＰＵ３０１から出力されるアドレスバス信号３１１とデータバス信号３２０と、ＣＰＵ３０１から出力される読み出し基準信号３１３（リード）と、レジスタ書き込み制御回路３０５の出力であるレジスタ書き込み信号３１９が入力される。

【００５７】

アクセス許可領域検出回路３０６は、メモリに対して読み出し及び書き込みの制約を解除するアドレス領域を設定するアクセス許可アドレス範囲設定レジスタ４０１と、アドレス比較回路４０２とによって構成される。アドレス領域（アクセス許可アドレス範囲）は、例えば、アドレス領域のスタートアドレスとエンドアドレスとを格納するレジスタを用意して設定する。このレジスタは、レジスタ書き込み信号３１９によって書き込みが行われる。但し、モニタフラグ３０４によって、上記特定アドレス空間からのみ書き込みが可能である。

【００５８】

このアクセス許可領域検出回路３０６においては、ＩＣカードのアプリケーションプログラムを実行する前に、オペレーティングシステムによってアプリケーションプログラムが格納されているアドレスのスタートアドレスとエンドアドレスが上記アクセス許可アドレス範囲設定レジスタにセットされる。アプリケーションプログラム実行中に、ＣＰＵ３０１から出力されるアドレスバス信号３１１とアクセス許可アドレス範囲設定レジスタ４０１の値とをアドレス比較回路４０２で比較することによって設定されたアドレス範囲をＣＰＵ３０１がアクセスしている間は、アドレス比較回路４０２からアクセス許可アドレス領域出力信号３１６に、「１」が出力される。また、同様にして、ＣＰＵ３０１が、実行中のア

プリケーションプログラム以外のアプリケーションプログラムが格納されている領域をアクセスした場合、アクセス許可アドレス領域出力信号３１６に、「０」が出力される。

【００５９】

アクセス許可設定レジスタ３０７には、ＣＰＵ３０１から出力されるアドレスバス信号３１１、データバス信号３２０、ＣＰＵ３０１から出力される読み出し基準信号３１３、及びレジスタ書き込み制御回路３０５の出力であるレジスタ書き込み信号３１９が入力される。

【００６０】

このアクセス許可設定レジスタ３０７は、アクセス許可領域検出回路３０６内のアクセス許可アドレス範囲設定レジスタ４０１に設定されたアドレス範囲外のアプリケーションプログラム領域に対して、読み出し又は書き込みのアクセスを許可するか否かを設定するレジスタである。このアクセス許可設定レジスタ３０７は、レジスタ書き込み信号３１９によって書き込みが行われる。但し、モニタフラグ３０４に基づいて、特定アドレス空間からのみ書き込み可能である。

【００６１】

ＩＣカードのアプリケーションプログラムを実行する前に、オペレーティングシステムによって、アクセス許可設定レジスタ３０７に「０」を設定したとき、アクセス許可信号３１７からは「０」が出力される。また、「１」を設定したとき、アクセス許可信号３１７からは「１」が出力される。

【００６２】

アクセス許可設定レジスタ３０７は、アクセス許可領域検出回路３０６内のアクセス許可アドレス範囲設定レジスタ４０１に設定したアドレス範囲外のアプリケーションプログラム領域に対して、読み出しまたは書き込みのアクセスを許可するか否かを設定するレジスタである。

【００６３】

上記のアクセス許可設定レジスタ３０７の設定内容が「０」のとき、アクセス許可領域検出回路３０６内のアクセス許可アドレス範囲設定レジスタ４０１で設定したアプリケーションプログラムアドレス範囲外は、読み出し、及び書き込み

が不可能となる。このアクセス許可設定レジスタ３０７の内容が「１」のときは、全てのアプリケーションプログラムメモリ領域は読み出し又は書き込みが可能となる。

【００６４】

メモリ読み出し制御回路３０９には、ＣＰＵ３０１から出力される読み出し基準信号３１３、アドレス比較回路４０２から出力されるアクセス許可アドレス領域出力信号３１６、及びアクセス許可信号３１７が入力される。このメモリ読み出し制御回路３０９は、ＡＮＤ回路４０３とセレクタ回路４０５により構成される。ここでは、読み出し基準信号３１３を不揮発性メモリ３０３に伝達するか否かの制御を行う。

【００６５】

アクセス許可信号３１７から「０」が出力されているとき、セレクタ回路４０５は、読み出し基準信号３１３とアクセス許可アドレス領域出力信号３１６をＡＮＤ回路４０３に入力して得られる信号を選択して、メモリ３０３へ読み出し信号３１８を与える。すなわち、アクセス許可領域検出回路３０６で設定したメモリ領域以外は、読み出し信号３１８を出力しない。アクセス許可信号３１７から「１」が出力されているとき、セレクタ回路４０５は、読み出し基準信号３１３を選択して、不揮発性メモリ３０３へ読み出し信号３１８を与える。すなわち、アプリケーションプログラムメモリ領域であれば、読み出し制限がなくなる。

【００６６】

メモリ書き込み制御回路３１０には、ＣＰＵ３０１から出力される書き込み基準信号３１２、アクセス許可アドレス領域出力信号３１６、及びアクセス許可信号３１７が入力される。このメモリ書き込み制御回路３１０は、ＡＮＤ回路４０４とセレクタ回路４０６とによって構成される。ここでは、書き込み基準信号３１２を不揮発性メモリ３０３に伝達するか否かの制御が行われる。

【００６７】

アクセス許可信号３１７から「０」が出力されているとき、セレクタ回路４０６は、書き込み基準信号３１２とアクセス許可アドレス領域出力信号３１６とをＡＮＤ回路４０４に入力して得られる信号を選択して、不揮発性メモリ３０３へ

書き込み信号３１５として出力する。即ち、アクセス許可領域検出回路３０６で設定したメモリ領域外（アドレス範囲外）は、書き込み信号を出力しない。アクセス許可信号３１７から「１」が出力されているとき、セレクタ回路４０６は、書き込み基準信号３１２を選択して、不揮発性メモリ３０３へ書き込み信号３１５として出力する。すなわち、アプリケーションプログラムメモリ領域であれば、書き込み制限がなくなる。

【００６８】

図４は、本実施の形態に係るアプリケーションプログラム格納用の不揮発性メモリ３０３のメモリマップ図である。この不揮発性メモリ３０３には、ｎ個のアプリケーションプログラムＡＰ１～ＡＰｎ（以下、単に、ＡＰ１～ＡＰｎと称す。）が格納されている。例えば、ＣＰＵ３０１がオペレーティングシステムにおいて、ＡＰ１のスタートアドレスとエンドアドレスをアクセス許可領域検出回路３０６のアクセス許可アドレス範囲設定レジスタ４０１にセットし、アクセス許可設定レジスタ３０７に「０」をセットしてＡＰ１を実行すると、ＡＰ１以外のアプリケーションプログラムメモリ領域は、アクセス不可となる。

【００６９】

図５は、ＣＰＵ３０１がＡＰ１を実行する前にオペレーティングシステムが行う処理のフローチャートである。まず、ステップＳ１、ステップＳ２によって、ＡＰ１のスタートアドレスとエンドアドレスをアクセス許可領域検出回路３０６のアクセス許可アドレス範囲設定レジスタ４０１にセットする。

【００７０】

次に、ステップＳ３によって、アクセス許可設定レジスタ３０７に「０」をセットする。次にステップＳ４によってＡＰ１への分岐命令を実行して、ＡＰ１の実行が開始される。ＡＰ１の実行が終了して、他のアプリケーションプログラムを実行する場合は、そのアプリケーションプログラムに対してステップＳ１～Ｓ４の動作を繰り返せばよい。これにより、異なるアプリケーションプログラムを他のアプリケーションプログラムに影響を与えることなく、連続的に実行することが可能となる。

【００７１】

また、アプリケーションプログラムメモリに、オペレーティングシステムによってアプリケーションプログラムが新たに追加されたり、入れ替えられた場合にも、そのアプリケーションプログラムのスタートアドレスとエンドアドレスを取得すれば、上記ステップを実行することができる。

【００７２】

図６は、１チップマイクロコンピュータにおいて、図２のブロック図のＣＰＵ３０１、メモリ保護回路５、不揮発性メモリ３０３について、詳細に記載したブロック図である。

【００７３】

この１チップマイクロコンピュータは、ＣＰＵ３０１とこれに含まれるプログラムカウンタ３０２、不揮発性メモリ３０３、モニタフラグ３０４、アクセス許可設定レジスタ３０７、アクセス許可アドレス範囲設定レジスタ４０１とアクセス許可設定レジスタ３０７に対する書き込み信号の発生を制限するレジスタ書き込み制御回路３０５、メモリに対して読み出し信号の発生を制限するメモリ読み出し制御回路３０９、メモリに対して書き込み信号の発生を制限するメモリ書き込み制御回路３１０、及び割り込み制御回路５２１とを備えている。

【００７４】

図６のメモリ読み出し制御回路３０９、メモリ書き込み制御回路３１０、及び割り込み制御回路５２１以外のブロックの動作は、図１のブロック図における動作内容と同一である。

【００７５】

メモリ読み出し制御回路３０９には、不揮発性メモリ３０３に対する不許可の読み出し動作が行われたことを示すメモリ読み出し違反検出信号５２２を出力する機能が追加されている。また、メモリ書き込み制御回路３１０には、不揮発性メモリ３０３に対する不許可の書き込み動作が行われたことを示すメモリ書き込み違反検出信号５２３を出力する機能が追加されている。

【００７６】

割り込み制御回路５２１は、メモリ読み出し制御回路３０９より出力されるメモリ読み出し違反検出信号５２２と、メモリ書き込み制御回路３１０から出力さ

れるメモリ書き込み違反検出信号５２３とを入力とし、ＣＰＵ３０１に対して割り込み要求信号５２４を出力する。

【００７７】

メモリ読み出し制御回路３０９に、「０」のアクセス許可信号３１７が入力されているとき、すなわち不揮発性メモリ３０３に対して読み出し及び書き込みの不許可が設定されているときに、アクセス許可アドレス領域検出回路３０６で許可したアドレス範囲外に対してＣＰＵ３０１が読み出し動作を行った場合、メモリ読み出し違反検出信号５２２が活性化される（アクティブになる）。

【００７８】

メモリ書き込み制御回路３１０に、「０」のアクセス許可信号３１７が入力されているとき、すなわち不揮発性メモリ３０３に対して読み出し及び書き込みの不許可が設定されているときに、アクセス許可アドレス領域検出回路３０６で許可したアドレス領域外に対してＣＰＵ３０１が書き込み動作を行った場合、メモリ書き込み違反検出信号５２３が活性化される。

【００７９】

それぞれのメモリアクセス違反検出信号は、割り込み制御回路５２１に入力されており、この回路からＣＰＵ３０１に対して割り込み要求信号５２４として伝達される。したがって、ＣＰＵ３０１は、実行中のアプリケーションプログラムが、それ以外のプログラムメモリの領域に対して不正アクセスしたときに、割り込み処理を行うことが可能になる。

【００８０】

不揮発性メモリ３０３への読み出しと書き込みとは同時に行われないので、割り込み制御回路５２１は、メモリ読み出し違反検出信号５２２及びメモリ書き込み違反検出信号５２３を入力とするＯＲ回路と、ＣＰＵ３０１の仕様に合わせてタイミングを制御する公知のタイミング制御回路（図示しない）とで構成でき、その出力で割り込み要求信号５２４を生成する。

【００８１】

図７は、上記メモリアクセス違反を検出して割り込み要求信号５２４が発生した場合のＣＰＵ３０１とオペレーティングシステムが管理する割り込み処理の一

例をフローチャートで表したものである。

【００８２】

ＣＰＵ３０１に割り込み要求信号５２４が入力されると、割り込み処理プログラムが起動される。まず、ステップＳ１１において、アクセス違反を起こしたアプリケーションプログラム（ＡＰ）の使用した作業領域などの初期化を行う。次に、ステップＳ１２においてアクセス違反を起こしたアプリケーションプログラム（ＡＰ）が再度実行されないように、オペレーティングシステムが管理する領域に用意された実行禁止を制御するフラグ又はレジスタをセットし、該アプリケーションプログラムが再度実行されることが禁止される。次に、ステップＳ１３においてオペレーティングシステムへのリターンアドレス（復帰アドレス）をセットし、割り込み処理を終了して、オペレーティングシステムへ制御が移る。

【００８３】

これにより、アプリケーションプログラムのアクセス違反が発生しても、ＣＰＵ３０１が暴走することなく処理を継続することが可能となる。上記ステップＳ１２においてフラグ又はレジスタが一旦セットされると、それ以降は、該アプリケーションプログラムが再度実行されることはない。つまり、フラグ又はレジスタがセットされていることが確認されると、該当するアプリケーションプログラムが再度実行されることはない。

【００８４】

図示はしないが、以上に詳述した１チップマイクロコンピュータをＩＣカードに搭載することによって、不揮発性メモリ３０３に複数のプログラムを格納でき、それぞれのプログラムを上述の従来技術のようにシステムをリセットすることなく動的に切り換えることができるので、そのＩＣカードをリーダライタに挿入した状態で多目的に利用できる。さらに、複数のプログラム及びデータ間の干渉を禁止できるため、不正なプログラムのアクセス防止やデータの保護等のセキュリティが確保できるため、個人情報等の機密データを格納するＩＣカードに適している。

【００８５】

上述の説明では、説明の便宜上、各種レジスタや各種フラグを例に挙げて説明

したが、本発明はこれに限定されるものではなく、同様の機能を有する記憶手段で代用してもよい。

【００８６】

本発明に係る１チップマイクロコンピュータは、以上のように、内蔵メモリとしてプログラム用メモリ及び作業用メモリを含むものであって、プログラムの実行命令のアドレスを指し示すプログラムカウンタを含むＣＰＵと、特定アドレス空間を実行していることを表すモニタフラグと、特定のアドレス空間からのみ設定が可能で、メモリに対して読み出しや書き込みのアクセス許可を設定するレジスタと、アクセスを許可するアドレス範囲を設定するレジスタと、内蔵メモリに対する読み出し信号、書き込み信号を制御する制御回路とを備えている。

【００８７】

上記発明によれば、アプリケーションプログラム格納用メモリのうち、実行中のアプリケーションプログラムが格納されている領域以外は、アクセス不可となり、他のアプリケーションプログラムが格納された領域に悪影響を及ぼすことがない。つまり、実行中のアプリケーションプログラムは、他のアプリケーションプログラムが格納された領域に悪影響を及ぼさない。また、オペレーティングシステムなどのシステムプログラム（システムソフトウェア）が格納された特定領域からのみ、アクセス許可レジスタとアドレス範囲設定レジスタへ設定できるため、これらのレジスタもアプリケーションプログラムから影響を受けない。つまり、特定アドレス空間からのみアクセス可能なアクセス許可レジスタ、アクセス範囲設定レジスタにも影響を与えない。

【００８８】

上記１チップマイクロコンピュータにおいて、特定領域からアクセス許可アドレス範囲設定レジスタやアクセス許可レジスタへデータを設定する手段を更に備えていることが好ましい。この場合、オペレーティングシステムからアプリケーションプログラムへ制御を移行する前に、アクセス可能とするアドレス範囲を設定でき、実行中のアプリケーションプログラムが他のアプリケーションプログラムへ影響を与えることがなくなる。

【００８９】

上記１チップマイクロコンピュータにおいて、実行中のアプリケーションプログラムが格納されているメモリ以外をアクセスしたとき、ＣＰＵへ割り込み要求信号を発生する手段を更に設けていることが好ましい。この場合、アプリケーションプログラムによって不正なアクセスがなされたとき、これを割り込み要求信号としてＣＰＵが検出できるため、ＣＰＵまたはアプリケーションプログラムの暴走を未然に防ぐことが可能となる。

【００９０】

上記１チップマイクロコンピュータにおいて、実行中のアプリケーションプログラムが格納されているメモリ以外をアクセスしたときに、ＣＰＵまたはアプリケーションプログラムの暴走を防ぐＣＰＵの割り込み処理プログラムを内蔵する構成が好ましい。この場合、アプリケーションプログラムによって不正なアクセスがなされたとき、割り込み処理プログラムを実行する（例えば、システムプログラムまたはオペレーティングシステムに制御を移す）ことによって、ＣＰＵまたはアプリケーションプログラムの暴走を防ぐことが可能となる。

【００９１】

上記１チップマイクロコンピュータにおいて、プログラムメモリがフラッシュメモリやＥＥＰＲＯＭなどの書き換え可能な不揮発性メモリであることが好ましい。この場合、アプリケーションプログラムを後から追加したり、書き換えたりしても、既存のアプリケーションプログラムに影響を与えることなく、プログラムを実行することができる。

【００９２】

上記１チップマイクロコンピュータにおいて、内蔵メモリ内へのアクセス制限を越えてアクセスが行われた場合に、アクセスを行ったプログラムの実行の禁止を制御する、システムプログラムまたはオペレーティングシステムが管理する領域に用意されたフラグまたはレジスタを有することが好ましい。この場合、アプリケーションプログラムを後から追加したり、書き換えたりしても、既存のアプリケーションプログラムに影響を与えることなく、プログラムを実行することが可能となる。一旦不正なアクセスを行ったプログラムは、以降、その実行が禁止されるため、ＣＰＵが暴走することなく処理を継続することが可能となる。

【００９３】

上記１チップマイクロコンピュータにおいて、プログラムメモリがフラッシュメモリやＥＥＰＲＯＭなどの書き換え可能な不揮発性メモリで構成することが好ましい。この場合、後から追加したり、書き換えたアプリケーションプログラムが、既存のアプリケーションプログラムに影響を与えることなく、プログラムを実行できる。

【００９４】

上記１チップマイクロコンピュータはＩＣカード用に好適である。この場合、複数のアプリケーションプログラムを内蔵したＩＣカードにおいて、アプリケーションプログラム間のセキュリティ性を確保することができる。また、複数のプログラムを格納するＩＣカードを実現でき、それぞれのプログラムをリセットすることなく動的に切り換えることができるので、そのＩＣカードをリーダライタに挿入した状態で多目的に利用できる。さらに、複数のプログラム及びデータ間の干渉を禁止できるため、不正なプログラムのアクセス防止やデータの保護等のセキュリティが確保できるので、個人情報等の機密データを格納するＩＣカードに適している。

【００９５】

【発明の効果】

本発明に係る１チップマイクロコンピュータは、特定アドレス空間を実行しているときに設定可能で、アクセスを許可するアドレス範囲を設定するアクセス許可アドレス範囲設定手段と、ソフトウェアの実行中に、設定された上記アドレス範囲内でアクセスされているか否かを判断する判断手段と、上記特定アドレス空間を実行しているときに設定可能で、上記アドレス範囲外のアドレスのアクセスを許可するか否かを設定するアクセス許可設定手段と、上記判断手段の結果と上記アクセス許可設定手段の設定内容とに基づいて、メモリに対するアクセスを制御する制御手段とを備えている。

【００９６】

上記の発明によれば、特定のアドレス空間に格納されたソフトウェアが実行されているときに、上記特定のアドレス空間からアクセス許可アドレス範囲設定手

段を介してアドレス範囲が設定できる。この場合、ソフトウェアの実行中に、該設定されたアドレス範囲内のアドレスに対してアクセスされているか否かが判断手段によって判断される。一方、上記特定のアドレス空間に格納されたソフトウェアが実行されていないときには、いくらデータが上記特定のアドレス空間からアクセス許可アドレス範囲設定手段に入力されていても、該データは該アクセス許可アドレス範囲設定手段に書き込まれることない。

【００９７】

一方、上記特定のアドレス空間に格納されたソフトウェアが実行されているときに、上記特定のアドレス空間からアクセス許可設定手段を介して上記アドレス範囲外のアドレスのアクセスを許可するか否かが設定できる。一方、上記特定のアドレス空間に格納されたソフトウェアが実行されていないときには、いくらデータが上記特定のアドレス空間からアクセス許可設定手段に入力されていても、該データは該アクセス許可設定手段に書き込まれることない。

【００９８】

上記判断手段の判断結果と、上記アクセス許可設定手段の設定内容とに基づいて、メモリに対するアクセスが制御手段によって制御される。すなわち、アドレス範囲が設定されていて、且つ、アドレス範囲外のアドレスのアクセスが許可されていないときには、メモリにおいて、該アドレス範囲内のアドレスに対してのみアクセス可能となる一方、該アドレス範囲外のアドレスに対してはアクセスはできない。

【００９９】

このようにメモリに対するアクセスを制御することによって、実行中のプログラムが他のプログラムが格納されているアドレス空間に悪影響を及ぼすことを未然に回避できる。また、特定のアドレス空間からのみ、アクセス許可設定手段とアドレス範囲設定手段とに対して設定ができるため、これらの設定手段もアプリケーションプログラムから影響を受けない。つまり、特定アドレス空間からのみアクセス可能なアクセス許可手段、アクセス範囲設定手段に対しても影響を与えないという効果を奏する。

【０１００】

本発明に係る他の１チップマイクロコンピュータは、特定アドレス空間を実行していることを表すフラグをセットするモニタフラグと、上記フラグがセットされているときに設定可能で、アクセスを許可するアドレス範囲を設定するアクセス許可アドレス範囲設定レジスタと、ソフトウェアの実行中に、設定された上記アドレス範囲内でアクセスされているか否かを判断する判断手段と、上記フラグがセットされているときに設定可能で、上記アドレス範囲外のアドレスのアクセスを許可するか否かを設定するアクセス許可設定レジスタと、上記判断手段の結果と上記アクセス許可設定レジスタの設定内容とに基づいて、メモリに対するアクセスを制御する制御手段とを備えている。

【０１０１】

上記の発明によれば、特定のアドレス空間に格納されたソフトウェアが実行されているときにフラグがモニタフラグによってセットされる。フラグがセットされているときに、アクセス許可アドレス範囲設定レジスタ及びアクセス許可設定レジスタの各レジスタに対して設定可能となる。

【０１０２】

フラグがセットされていないときには、特定のアドレス空間に格納されたソフトウェアが実行されていないので、モニタフラグはフラグをセットしない。したがって、このとき、たとえ上記特定のアドレス空間から設定しても、アクセス許可アドレス範囲設定レジスタ及びアクセス許可設定レジスタの各レジスタに対する設定はできなくなる。

【０１０３】

上記フラグがセットされているときに、上記特定のアドレス空間からアクセス許可アドレス範囲設定レジスタを介して、アドレス範囲が設定できる。この場合、ソフトウェアの実行中に、該設定されたアドレス範囲内のアドレスに対してアクセスされているか否かが判断手段によって判断される。これに対して、上記フラグがセットされていないときに、いくらデータが上記特定のアドレス空間からアクセス許可アドレス範囲設定レジスタに入力されていても、該データは該アクセス許可アドレス範囲設定レジスタに書き込まれることない。

【０１０４】

一方、上記フラグがセットされているときに、上記特定のアドレス空間からアクセス許可設定レジスタを介して、上記アドレス範囲外のアドレスのアクセスを許可するか否かが設定できる。これに対して、上記フラグがセットされていないときには、いくらデータが上記特定のアドレス空間からアクセス許可設定レジスタに入力されていても、該データは該アクセス許可設定レジスタに書き込まれることない。

【０１０５】

上記判断手段の判断結果と、上記アクセス許可設定レジスタの設定内容とに基づいて、メモリに対するアクセスが制御手段によって制御される。すなわち、アドレス範囲が設定されていて、且つ、アドレス範囲外のアドレスのアクセスが許可されていないときには、メモリにおいて、該アドレス範囲内のアドレスに対してのみアクセス可能となる一方、該アドレス範囲外のアドレスに対してはアクセスはできない。

【０１０６】

このようにメモリに対するアクセスを制御することによって、実行中のプログラムが他のプログラムが格納されているアドレス空間に悪影響を及ぼすことを未然に回避できる。また、特定のアドレス空間からのみ、アクセス許可設定レジスタとアドレス範囲設定レジスタとに対して設定ができるため、これらのレジスタもアプリケーションプログラムから影響を受けない。つまり、特定アドレス空間からのみアクセス可能なアクセス許可レジスタ、アクセス範囲設定レジスタにも影響を与えない。また、アドレス範囲が設定されていて、且つ、アドレス範囲外のアドレスのアクセスが許可されているときには、該アドレス範囲外のアドレスに対してもアクセス可能となるという効果を併せて奏する。

【０１０７】

上記１チップマイクロコンピュータにおいて、上記特定のアドレス空間には、システムソフトウェアが格納されており、該システムソフトウェアは、次のプログラムを実行する前に、該プログラムの格納されているアドレス範囲を上記アクセス許可アドレス範囲設定レジスタに設定すると共に、該アドレス範囲外のアドレスに対してアクセスを許可しないように上記アクセス許可レジスタを設定する

ことが好ましい。

【０１０８】

この場合、次のプログラムが実行されるのに先立って、システムソフトウェアは、この実行しようとしている次のプログラムの格納されているアドレス範囲をアクセス許可アドレス範囲設定レジスタに設定する。つまり、実行中のプログラムは、次に実行するプログラムのアドレス範囲が設定されるまで、該次に実行するプログラムをアクセスすることはない。

【０１０９】

これにより、オペレーティングシステムなどのシステムソフトウェアからアプリケーションプログラム等の次に実行されるプログラムへ制御が移行される前に、アクセス可能とするアドレス範囲を設定できる。したがって、実行中のプログラムが次に実行されるプログラムに影響を与えることを未然に回避でき、信頼性が著しく向上するという効果を奏する。

【０１１０】

上記１チップマイクロコンピュータにおいて、上記アドレス範囲外のアドレスのアクセスを不許可とする設定がアクセス許可設定レジスタになされており、上記アドレス範囲外のアドレスに対してアクセスしたことが判断手段によって判断されたとき、割り込み要求信号を生成してＣＰＵへ送る割り込み要求信号生成手段を更に備え、所定の割り込み処理プログラムを実行することが好ましい。

【０１１１】

この場合、他のプログラムによって不正なアクセスがなされたとき、アドレス範囲外のアドレスに対してアクセスしたことが判断手段によって判断され、割り込み要求信号生成手段によって割り込み要求信号が生成されてＣＰＵへ送られる。ＣＰＵは、この割り込み要求信号を受領すると、所定の割り込み処理プログラムが実行されるので、ＣＰＵが暴走することを未然に防ぐことができるという効果を奏する。

【０１１２】

上記１チップマイクロコンピュータにおいて、上記割り込み処理プログラムは、システムプログラムまたはオペレーティングシステムに制御を移すプログラム

であることが好ましい。

【０１１３】

この場合、割り込み要求信号生成手段によって割り込み要求信号が生成されてＣＰＵへ送られると、割り込み処理プログラムが実行され、システムプログラムまたはオペレーティングシステムに制御が移される。これにより、ＣＰＵまたはアプリケーションプログラムの暴走を防ぐことが可能となるという効果を奏する。

【０１１４】

上記１チップマイクロコンピュータにおいて、上記システムソフトウェアが管理する領域に設けられ、メモリへのアクセス制限を越えてアクセスが行われた場合にその旨の情報を記憶する再実行禁止情報記憶手段を更に備え、該情報に基づいて、上記制御手段は上記メモリを制御し、アクセス制限を越えて上記アクセスが再度行われないようにすることが好ましい。

【０１１５】

この場合、メモリへのアクセス制限を越えてアクセスが行われると、その旨の情報が再実行禁止情報記憶手段（例えば、フラグやレジスタ等）に記憶されることになる。上記制御手段は、この情報に基づいて上記メモリを制御し、アクセス制限を越えて上記アクセスが再度行われないようにする。これにより、一旦不正なアクセスが行われたプログラムに対しては、それ以降、その実行が禁止されるので、ＣＰＵは、暴走することなく処理を継続して行うことが可能となるという効果を奏する。

【０１１６】

上記１チップマイクロコンピュータにおいて、上記メモリは、書き換え可能な不揮発性メモリであることが好ましい。

【０１１７】

この場合、後から追加したり、書き換えたりしたプログラム（例えば、アプリケーションプログラム）等が既存のプログラムに影響を与えることなく実行することができるという効果を奏する。

【０１１８】

上記の１チップマイクロコンピュータは、ＩＣカードに適用することが好ましい。

【０１１９】

この場合、複数のアプリケーションプログラムを内蔵したＩＣカードにおいて、アプリケーションプログラム間のセキュリティ性を確実に確保することができる。また、複数のプログラムを格納するＩＣカードを実現でき、それぞれのプログラムをリセットすることなく動的に切り換えることができるので、そのＩＣカードをリーダライタに挿入した状態で多目的に利用できる。さらに、複数のプログラム及びデータ間の干渉を禁止できるため、不正なプログラムのアクセス防止やデータの保護等のセキュリティ性が確保できるので、個人情報等の機密データを格納するＩＣカードに適しているという効果を併せて奏する。

【図面の簡単な説明】

【図１】

本発明の１チップマイクロコンピュータの構成例を示すブロック図である。

【図２】

上記１チップマイクロコンピュータの具体例を示すブロック図である。

【図３】

アクセス許可領域検出回路とアクセス制御回路周辺の構成例を示すブロック図である。

【図４】

本発明に係る１チップマイクロコンピュータのアプリケーションプログラム用メモリのメモリマップ図である。

【図５】

上記アプリケーションプログラムの分岐時のフローチャートである。

【図６】

本発明の１チップマイクロコンピュータの構成例を示すブロック図である。

【図７】

メモリ不正アクセス時の割り込み処理フローチャートである。

【図８】

従来の１チップマイクロコンピュータの構成例を示すブロック図である。

【図９】

従来のＣＰＵの構成機能図である。

【符号の説明】

３０１　ＣＰＵ

３０２　プログラムカウンタ

３０３　不揮発性メモリ

３０４　モニタフラグ

３０５　レジスタ書き込み制御回路

３０６　アクセス許可領域検出回路

３０７　アクセス許可設定レジスタ

３０８　命令取り出し信号

３０９　メモリ読み出し制御回路

３１０　メモリ書き込み制御回路

３１１　アドレスバス信号

３１２　書き込み基準信号

３１３　読み出し基準信号

３１４　モニタフラグ出力信号

３１５　メモリ書き込み信号

３１６　アクセス許可アドレス範囲設定レジスタ出力信号

３１７　アクセス許可設定レジスタ出力信号

３１８　メモリ読み出し信号

３１９　レジスタ書き込み信号

３２０　データバス信号

４０１　アクセス許可アドレス範囲設定レジスタ

４０２　アドレス比較回路

４０３　ＡＮＤ回路

４０５　セレクタ回路

５２１　割り込み制御回路

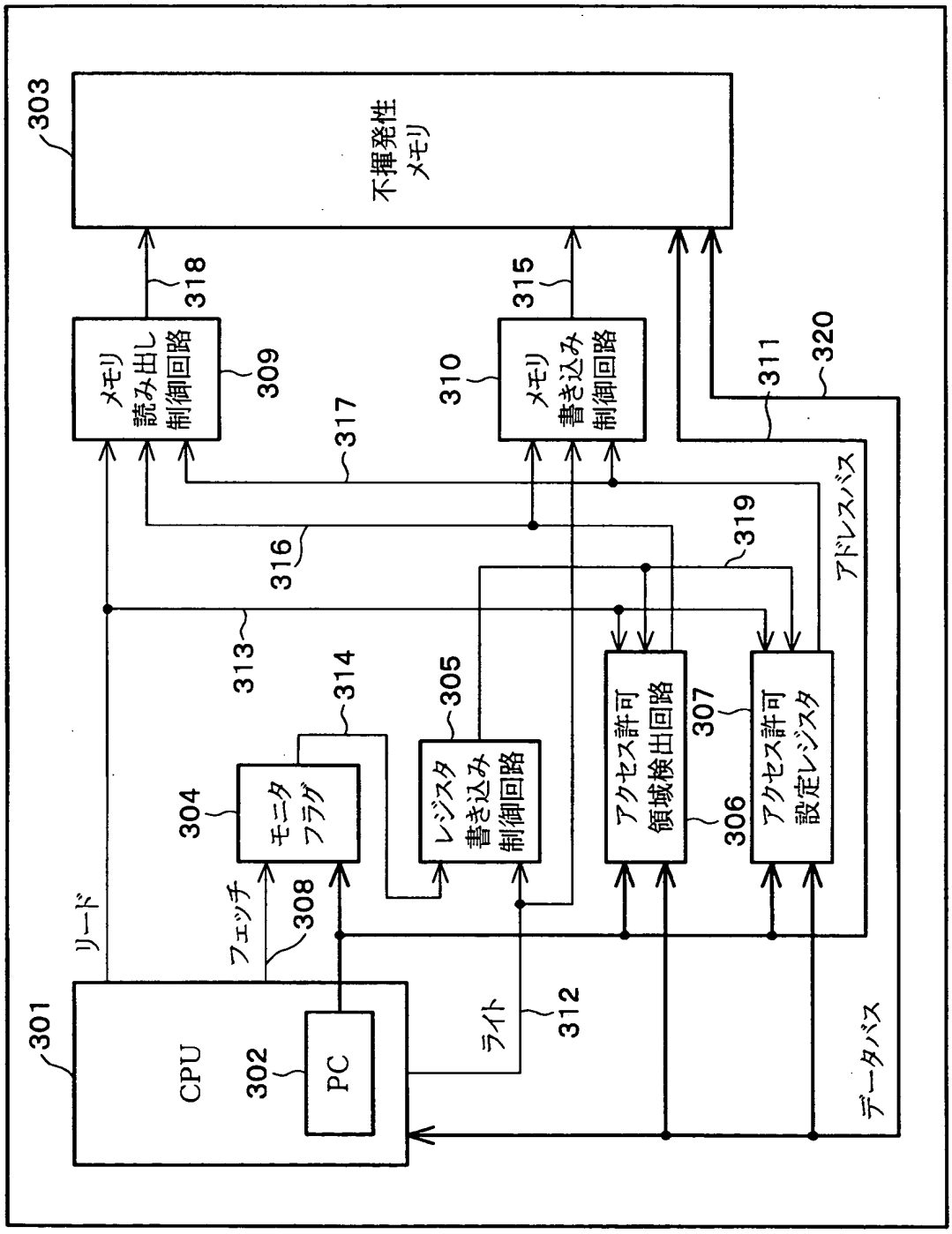
５２２　メモリ読み出し違反検出信号

５２３　メモリ書き込み違反検出信号

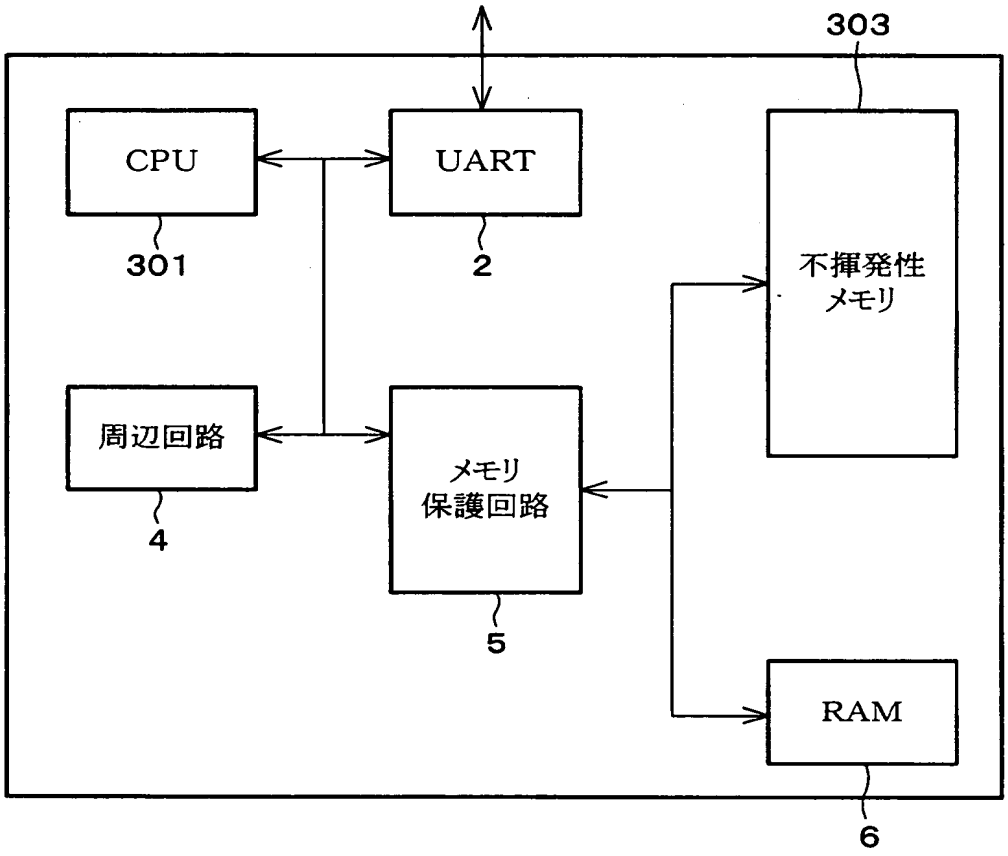
５２４　割り込み要求信号

【書類名】　図面

【図１】

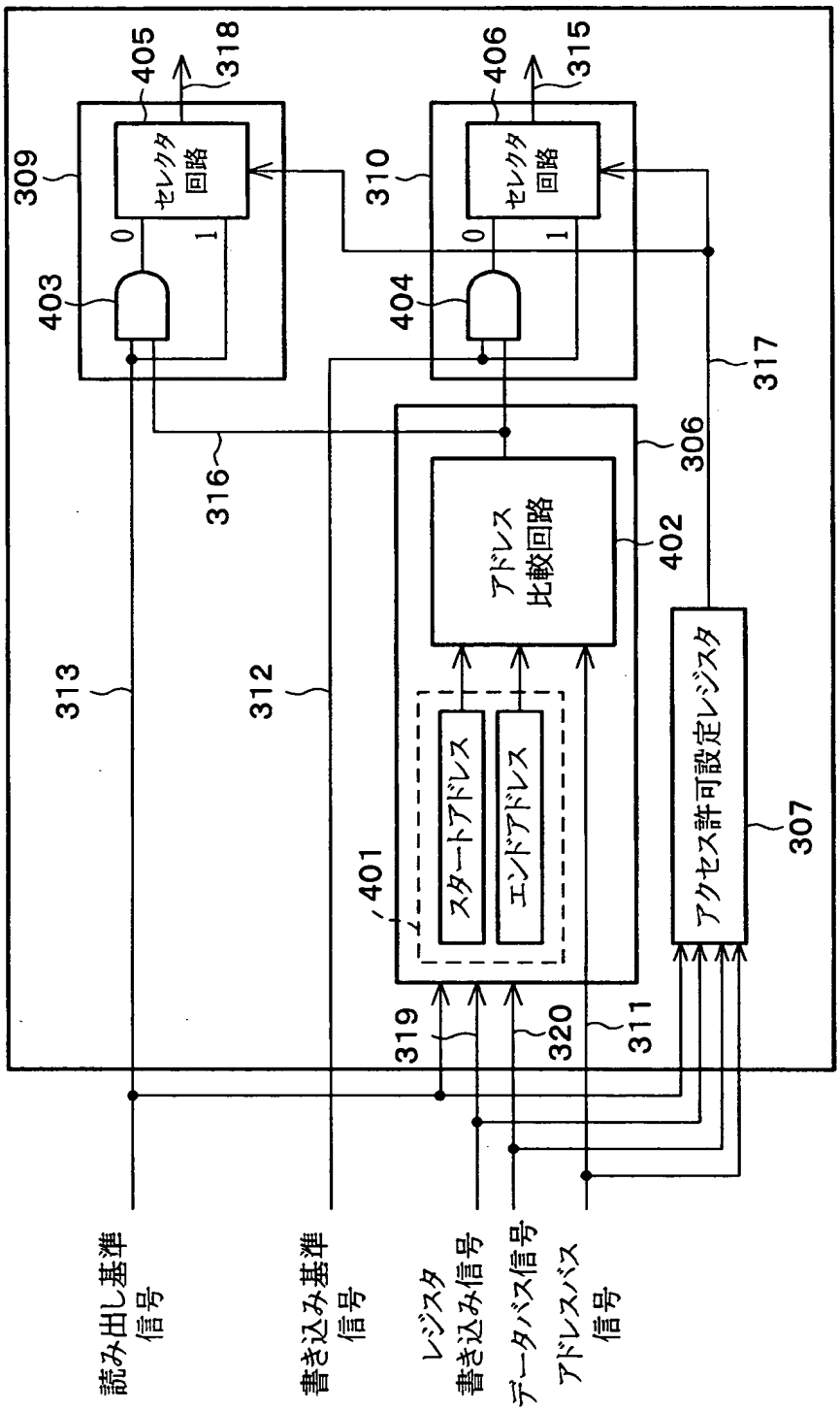

303
不揮発性メモリ
318
メモリ読み出し制御回路
309
317
315
メモリ書き込み制御回路
310
311
320
316
319
アドレスバス
313
314
305
304
モニタフラグ
レジスタ書き込み制御回路
アクセス許可領域検出回路
307
アクセス許可設定レジスタ
306
リード
フェッチ
308
301
CPU
302
PC
ライト
312
データバス

【図２】

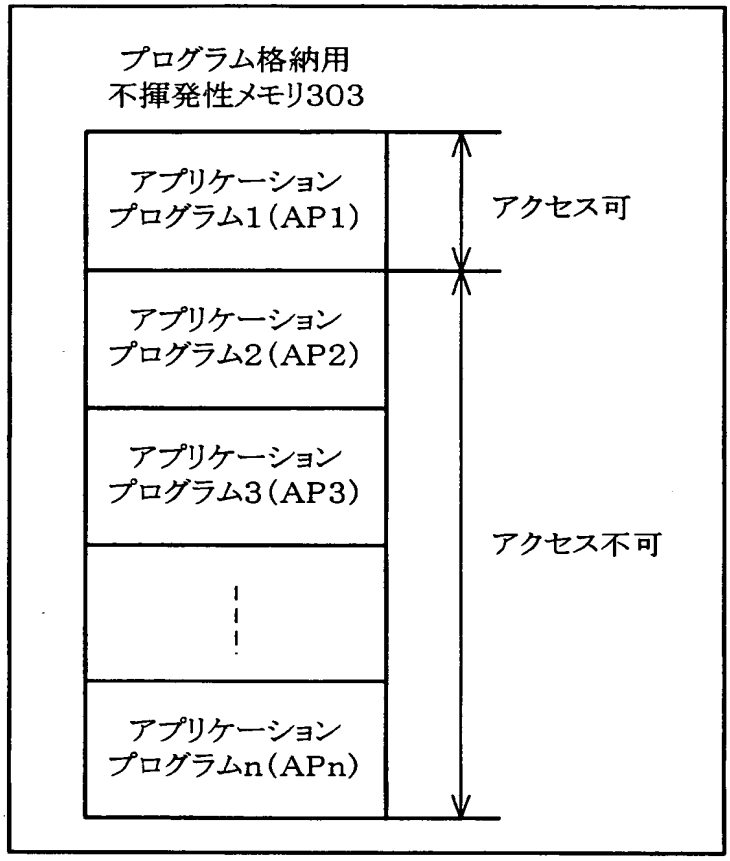


出証特２００１－３００６０１５

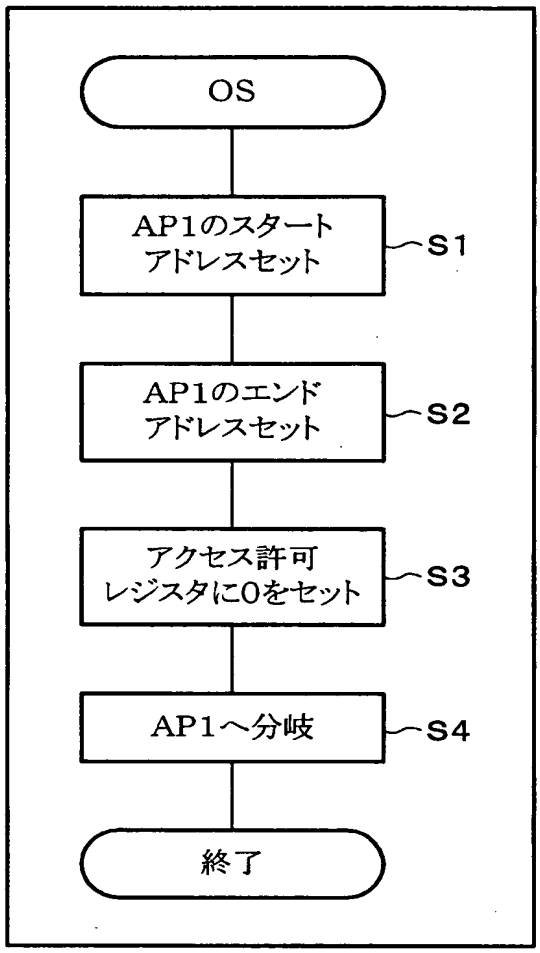
【図３】


405
318
406
315
309
セレクタ回路
310
セレクタ回路
0
1
0
1
403
404
317
316
306
アドレス比較回路
402
313
312
401
スタートアドレス
エンドアドレス
アクセス許可設定レジスタ
307
319
320
311
読み出し基準信号
書き込み基準信号
レジスタ書き込み信号
データバス信号
アドレスバス信号

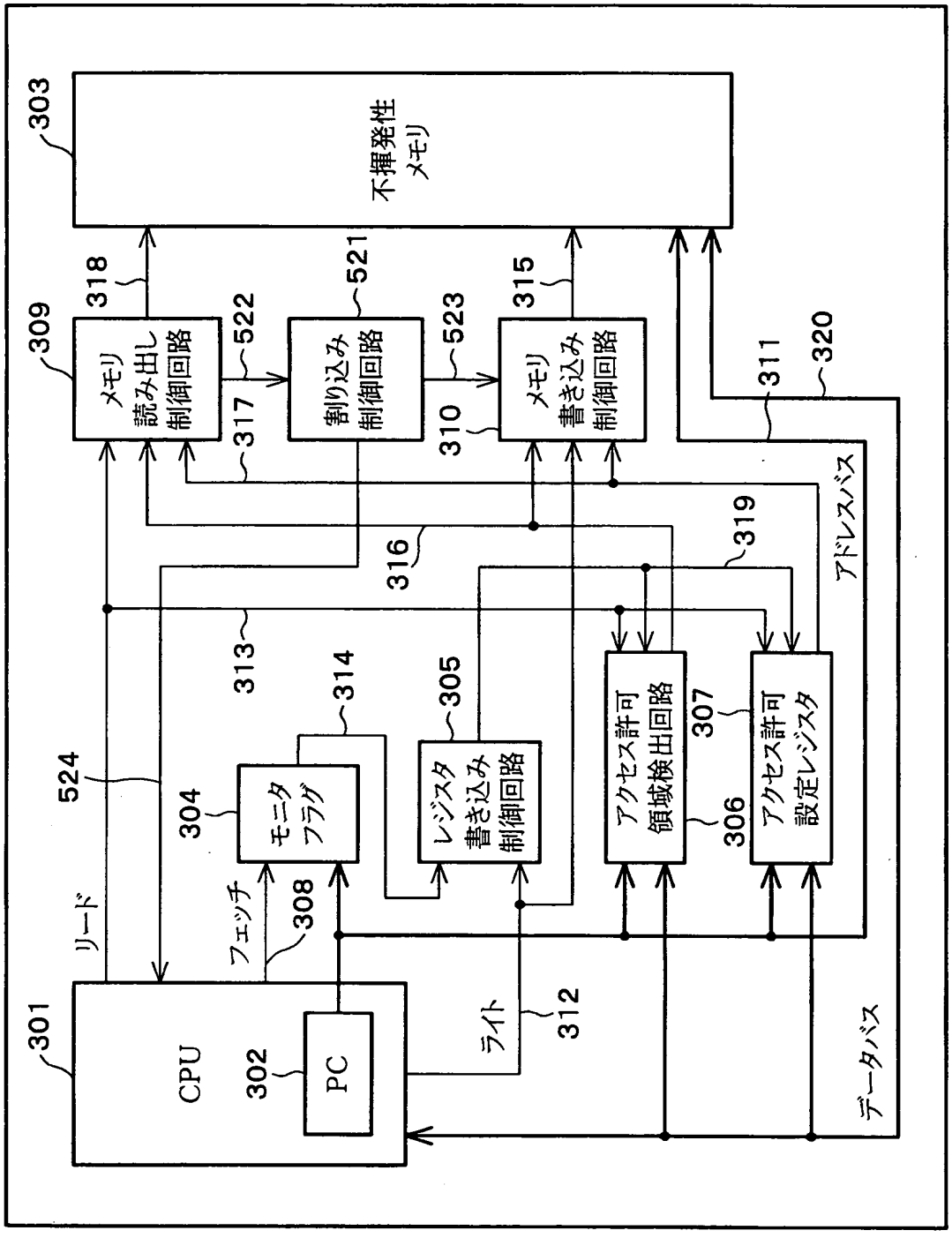
【図４】


プログラム格納用
不揮発性メモリ303
アプリケーション
プログラム1(AP1)
アプリケーション
プログラム2(AP2)
アプリケーション
プログラム3(AP3)
アプリケーション
プログラムn(APn)
アクセス可
アクセス不可

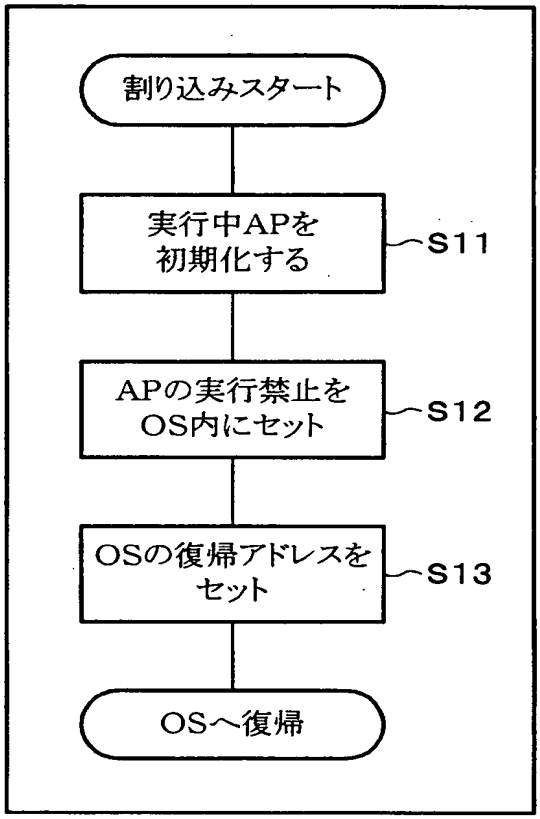
【図５】


OS
AP1のスタート
アドレスセット
S1
AP1のエンド
アドレスセット
S2
アクセス許可
レジスタに0をセット
S3
AP1へ分岐
S4
終了

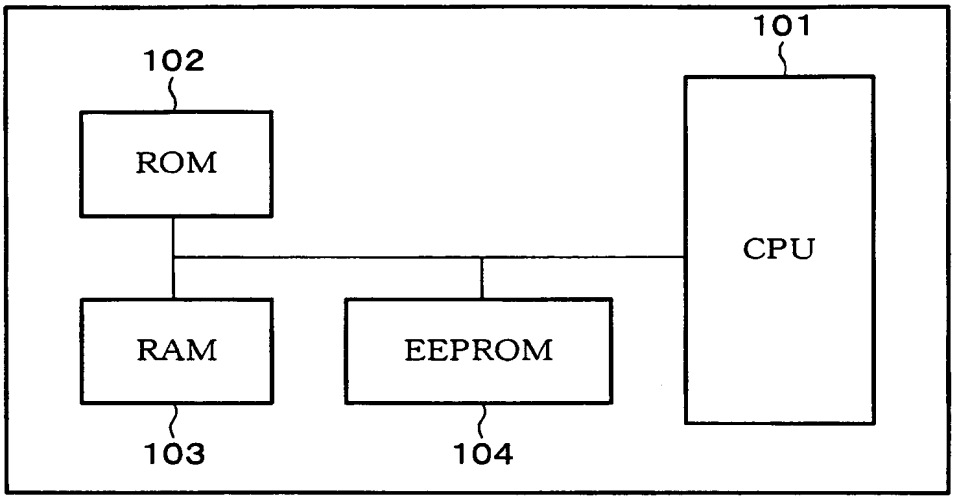
【図６】


303
不揮発性メモリ
318
309
メモリ読み出し制御回路
522
521
割り込み制御回路
523
315
メモリ書き込み制御回路
311
320
317
310
316
319
アドレスバス
313
314
305
524
304
モニタフラグ
レジスタ書き込み制御回路
アクセス許可領域検出回路
307
アクセス許可設定レジスタ
306
リード
フェッチ
308
ライト
312
301
CPU
302
PC
データバス

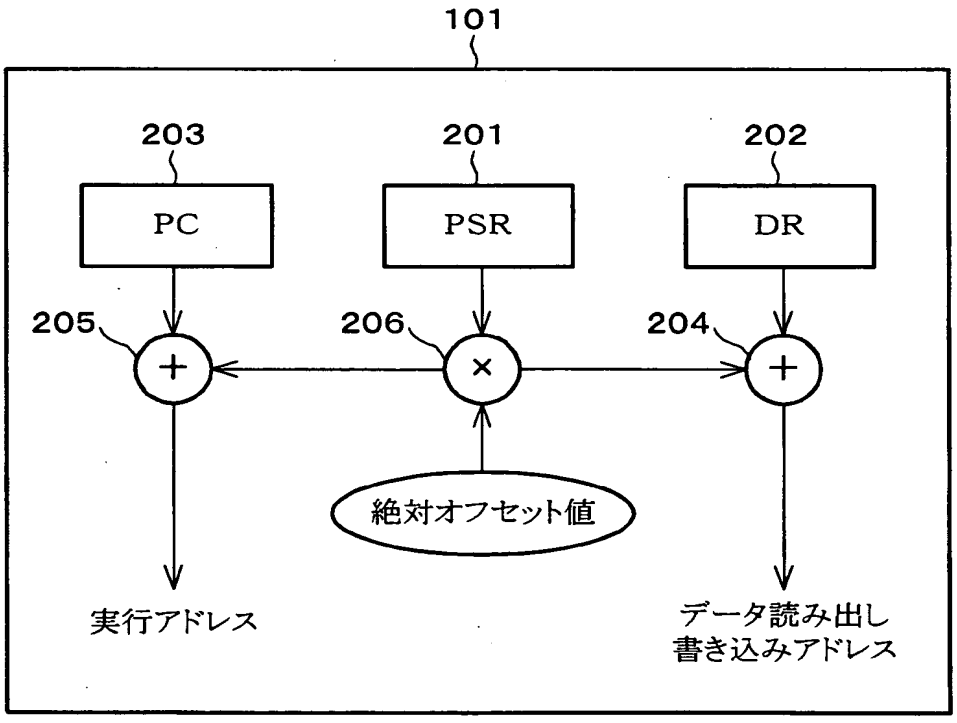
【図７】


割り込みスタート
実行中APを
初期化する
S11
APの実行禁止を
OS内にセット
S12
OSの復帰アドレスを
セット
S13
OSへ復帰

【図８】


101
102
ROM
CPU
RAM
EEPROM
103
104

【図９】


101
203
201
202
PC
PSR
DR
205
206
204
絶対オフセット値
実行アドレス
データ読み出し
書き込みアドレス

【書類名】　要約書

【要約】

【課題】　アプリケーションプログラム間のセキュリティ性を確保した１チップマイクロコンピュータを提供する。

【解決手段】　本発明の１チップマイクロコンピュータは、特定アドレス空間を実行していることを表すフラグをセットするモニタフラグ３０４と、上記フラグがセットされているときにアクセスを許可するアドレス範囲を設定するアクセス許可アドレス範囲設定レジスタと、設定された上記アドレス範囲内でアクセスされているか否かを判断するアクセス許可領域検出回路３０６と、上記アドレス範囲以外のアドレスのアクセスを許可するか否かを設定するアクセス許可設定レジスタ３１９と、上記判断結果と上記アクセス許可設定レジスタ３１９の設定内容とに基づいて、不揮発性メモリ３０３に対するアクセスを制御するメモリ読み出し制御回路３０９及びメモリ書き込み回路３１０とを備えている。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５０４９〕

１．変更年月日　　１９９０年　８月２９日
［変更理由］　新規登録
住　所　　大阪府大阪市阿倍野区長池町２２番２２号
氏　名　　シャープ株式会社

出 願 人 履 歴 情 報

識別番号　　〔０００００４２２６〕

１．変更年月日　　１９９９年　７月１５日
　〔変更理由〕　　住所変更
　　住　所　　東京都千代田区大手町二丁目３番１号
　　氏　名　　日本電信電話株式会社